CAA restrictions

The question

Know who issues your certificates

CAA publishes certificate issuance instructions in DNS. Your policy should match every platform that obtains certificates for your domain.

01 Understand

02 Observe

03 Verify

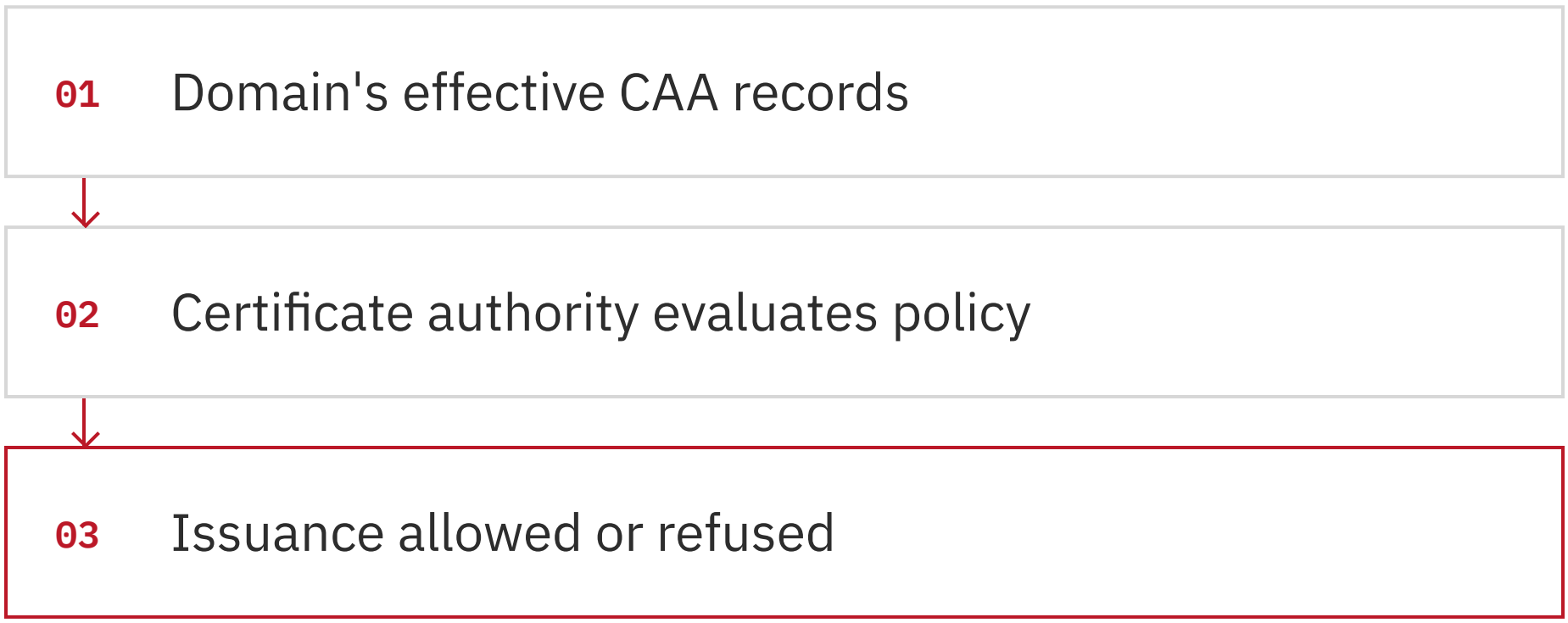
A practical briefing for the people who own your domain.

CAA restrictions

The mechanism

Certificate type changes the rule

issue covers ordinary issuance. issuewild governs wildcard issuance when present. Wildcard-only publication leaves ordinary issuance unrestricted.



The scanner observes the publication stage. It does not request a certificate or validate an authority's issuance decision.

CAA restrictions

The evidence

We observe recognised publication

> Our check finds issue or issuewild forms. It does not validate provider suitability or prove that every issuance path is restricted.

PUT THE OBSERVATION IN CONTEXT

Public signal

Service context

Operational validation

Use the finding to start an owned review.

CAA restrictions

The handoff

Inventory before restricting

Ask certificate and hosting owners which authorities they require. Include managed renewal and backup providers before changing DNS.

BRING THE RIGHT OWNERS TOGETHER

01 Certificate and web platform owners

02 DNS administrator with certificate operations

CAA restrictions

Your checklist

Use the CAA review checklist

- ✓ List authorities
- ✓ Review wildcard scope
- ✓ Check inheritance
- ✓ Test renewal

> Read the CAA explainer and assign policy ownership.
>
> **/learn/caa**